Midterm Examination
Coding Theory

27^{th} January 2006

Time: 2 hours (12:30–2:30pm)

1. Our task is to design a Hamming code in the case where there are 4 check digits. First find the binary-representative matrix M to be used for the purpose.[1]† Find the length of the code word [1] and that of a message word [1]. What is the redundancy of this code?[1] Then construct the code.[5] And then code the message words 10101010101 [3] and 00111100101 [3].

Solution. We have $r = 4$, $n = 2^4 - 1 = 15$ and $m = 2^4 - 4 - 1 = 11$. Each code word has 15 digits and 4 check digits.

#

Each message The redundancy of the code is 4.

#

check digits	b_1	b_2		b_4				b_8							
	$\uparrow$	$\uparrow$		$\uparrow$				$\uparrow$							
code word	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
			$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
message word			a_1		a_2	a_3	a_4		a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}

The $(2^r - 1) \times r$ matrix M is then

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Then form the matrix equation

$$(\, b_1 \quad b_2 \quad \cdots \quad b_{15} \,)\, M = \mathbf{0}$$

which gives four equations in four unknown,

$$\begin{aligned} b_8 + b_9 + b_{10} + b_{11} + b_{12} + b_{13} + b_{14} + b_{15} &= 0 \\ b_4 + b_5 + b_6 + b_7 + b_{12} + b_{13} + b_{14} + b_{15} &= 0 \\ b_2 + b_3 + b_6 + b_7 + b_{10} + b_{11} + b_{14} + b_{15} &= 0 \\ b_1 + b_3 + b_5 + b_7 + b_9 + b_{11} + b_{13} + b_{15} &= 0 \end{aligned}$$

The message word 10101010101 becomes the code word

$$b_1 \quad b_2 \quad 1 \quad b_4 \quad 0 \quad 1 \quad 0 \quad b_8 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1$$

† Numbers placed between square brackets are marks.

Hence, $b_8 = 0$, $b_4 = 1$, $b_2 = 0$ and $b_1 = 1$, and the code word is 101101001010101.

#

The message 00111100101 becomes the code word

$$b_1 \quad b_2 \quad 0 \quad b_4 \quad 0 \quad 1 \quad 1 \quad b_8 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1$$

which gives us $b_8 = 0$, $b_4 = 0$, $b_2 = 0$ and $b_1 = 1$. Therefore the code word is 100001101100101.

#

2. Show that the polynomial $x^3 + x^2 + 1$ is irreducible [4] and the element $\alpha = x + \langle x^3 + x^2 + 1 \rangle$ of $F[x]/\langle x^3 + x^2 + 1 \rangle$ primitive [4]. Then use this to construct a binary BCH code of length 7 and minimum distance 3.[5] And then find the code word for the message 1101.[2]

Solution. Suppose $x^3 + x^2 + 1$ is reducible, then it must have either x or $x + 1$ as a factor, then $x = 0$ or 1 is a root of $x^3 + x^2 + 1$. But

$$\begin{array}{r|l} & x^2 + x \\ \hline x & x^3 + x^2 + 1 \\ & x^3 \\ \hline & x^2 + 1 \\ & x^2 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} & x^2 \\ \hline x + 1 & x^3 + x^2 + 1 \\ & x^3 + x^2 \\ \hline & 1 \end{array}$$

from which we can see that both $x | x^3 + x^2 + 1$ and $x + 1 | x^3 + x^2 + 1$ give a remainder 1. Therefore neither x nor $x + 1$ divides $x^3 + x^2 + 1$, hence the latter is irreducible.

#

We know that $f(x)$ in $F_p[x]$ of degree n is primitive if $f(x) | x^{p^n - 1} - 1$ and $f(x) \not| x^k - 1$ for any $k < p^n - 1$. We have $x^{2^3 - 1} - 1 = x^7 - 1$. Then

$$\begin{array}{r|l} & x^4 + x^3 + x^2 + 1 \\ \hline x^3 + x^2 + 1 & x^7 - 1 \\ & x^7 + x^6 + x^4 \\ \hline & x^6 + x^4 + 1 \\ & x^6 + x^5 + x^3 \\ \hline & x^5 + x^4 + x^3 + 1 \\ & x^5 + x^4 + x^2 \\ \hline & x^3 + x^2 + 1 \quad \to 0 \end{array} \quad \Rightarrow \quad x^3 + x^2 + 1 | x^7 - 1$$

For $k < 7$; if $k = 6$;

$$\begin{array}{r|l} & x^3 + x^2 + x \\ \hline x^3 + x^2 + 1 & x^6 - 1 \\ & x^6 + x^5 + x^3 \\ \hline & x^5 + x^3 + 1 \\ & x^5 + x^4 + x^2 \\ \hline & x^4 + x^3 + x^2 + 1 \\ & x^4 + x^3 + x \\ \hline & x^2 + x + 1 \quad \neq 0 \end{array} \quad \Rightarrow \quad x^3 + x^2 + 1 \not| x^6 - 1$$

If $k = 5$;

$$
\begin{array}{r|l}
 & x^2+x+1 \\
\hline
x^3+x^2+1 & x^5-1 \\
 & x^5+x^4+x^2 \\
\hline
 & x^4+x^2+1 \\
 & x^4+x^3+x \\
\hline
 & x^3+x^2+x+1 \\
 & x^3+x^2+1 \\
\hline
 & x \neq 0
\end{array}
\quad \Rightarrow \quad x^3+x^2+1 \not| x^5-1
$$

If $k=4$;

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^3+x^2+1 & x^4-1 \\
 & x^4+x^3+x \\
\hline
 & x^3+x+1 \\
 & x^3+x^2+1 \\
\hline
 & x^2+4 \neq 0
\end{array}
\quad \Rightarrow \quad x^3+x^2+1 \not| x^4-1
$$

When $k=3$, $x^3+x^2+1 \not| x^3-1$ is obvious. Therefore $\alpha = x + \langle x^3+x^2+1 \rangle$ is a primitive of $F[x]/\langle x^3+x^2+1 \rangle$.

Then, α satisfies $\alpha^3+\alpha^2+1=0$. For F a finite field of order p^n with k as its prime subfield, we know that α and α^p have the same minimum polynomial over k for every $\alpha \in F$. Here $p=1$; therefore α and α^2 have the same minimum polynomial, hence the generating polynomial is x^3+x^2+1. Let the message be $a_0a_1a_2a_3$. Then the message polynomial is $a(x)=a_0+a_1x+a_2x^2+a_3x^3$. The corresponding code polynomial is therefore $a(x)\left(x^3+x^2+1\right)$. In other words,

$$a_0+a_1x+(a_0+a_2)\,x^2+(a_0+a_1+a_3)\,x^3+(a_1+a_2)\,x^4+(a_2+a_3)\,x^5+a_3x^6$$

The code word is thus

$$(a_0, a_1, (a_0+a_2), (a_0+a_1+a_3), (a_1+a_2), (a_2+a_3), a_3)$$

#

For the message 1101, the code word is 1111111.

#